



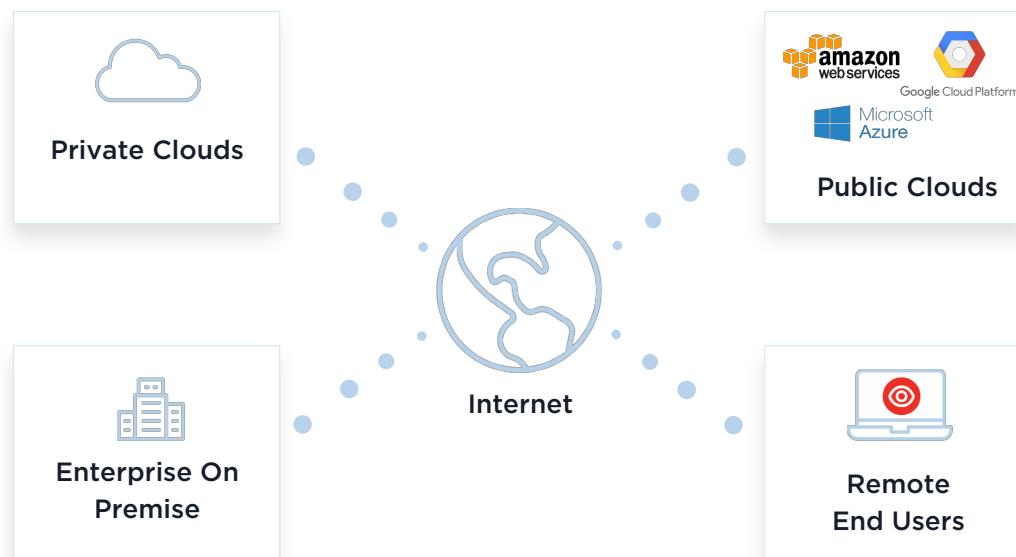
QUALYS SECURITY CONFERENCE 2018

Cloud Agent Platform

Chris Carlson

VP, Product Management, Qualys, Inc.

Digital Transformation is Driving IT Transformation for Organizations



... But creates new Challenges for Security

Don't know how many assets you have



Don't know when those assets are running



Credential issues / Authentication failures



Monthly / weekly scanning too slow [WannaCry]

Enterprise On Premise

Remote End Users

Can't scan remote users

Qualys Sensors

Scalable, self-updating & centrally managed

					
Physical	Virtual	Cloud/Container	Cloud Agents	Passive	API
Legacy data centers	Private cloud infrastructure	Commercial IaaS & PaaS clouds	Light weight, multi-platform	Passively sniff on network	Integration with Threat Intel feeds
Corporate infrastructure	Virtualized Infrastructure	Pre-certified in market place	On premise, elastic cloud & endpoints	Real-time device discovery & identification	CMDB Integration
Continuous security and compliance scanning	Continuous security and compliance scanning	Fully automated with API orchestration	Real-time data collection	Identification of APT network traffic	Log connectors
		Continuous security and compliance scanning	Continuous evaluation on platform for security and compliance	Extract malware files from network for analysis	

Qualys Cloud Agent Platform



**Lightweight
Software
Agent**

(collects metadata only)



**On-Premise
Servers**
Public Cloud
**User
Endpoints**

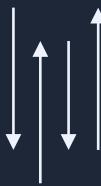


Windows
Linux
Mac
AIX
Cloud Native



**Delivers
Multiple
Security
Functions in
one Agent**

Qualys Platform

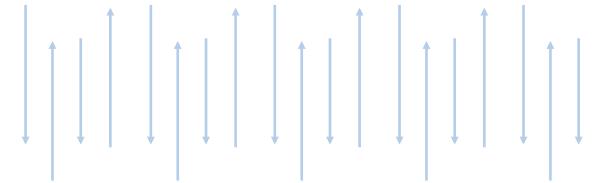


Cloud Agent

Central Management / API



Qualys Suite of
Applications



Efficient Network Usage
(*Delta Processing average*)

50 - 350 KB / day

Lightweight Metadata
Collection (*tunable*)

~1-2% CPU

Windows, Linux, Mac, AIX

3 MB application

Qualys Cloud Agent

IT, Security, Compliance Apps

AI Asset Inventory

VM Vulnerability Management

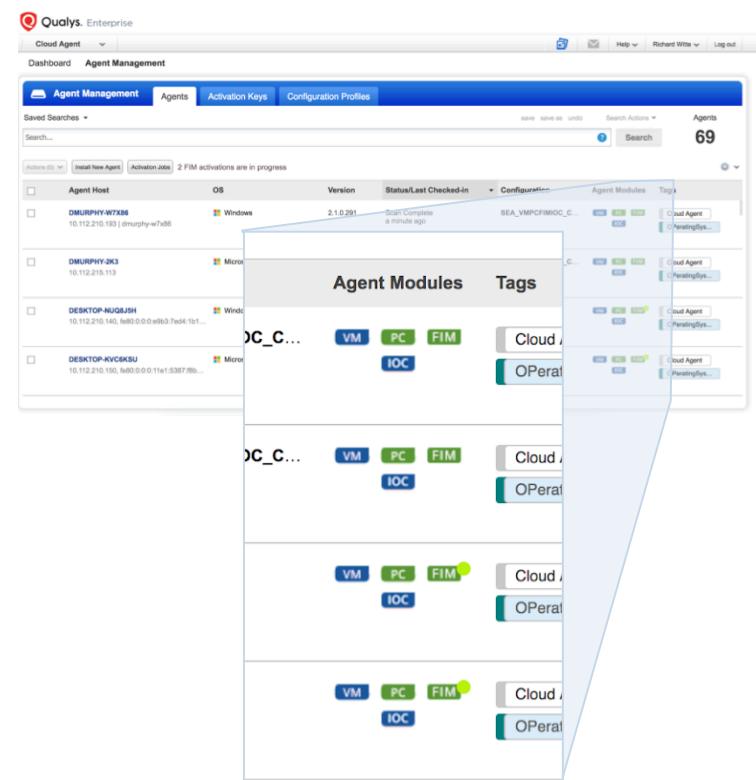
PC Policy Compliance

IOC Indication of Compromise Detection

FIM File Integrity Monitoring

Upcoming IT App (Beta November 2018)

PM Patch Management



Try and Manage Apps on One Cloud Agent

End the fight with IT to deploy security agents!

Remove point-solution agents from your endpoints

Consolidate security tools

Activation Key Turn help tips: On | Off 

Edit the activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title [Select](#) | [Create](#)



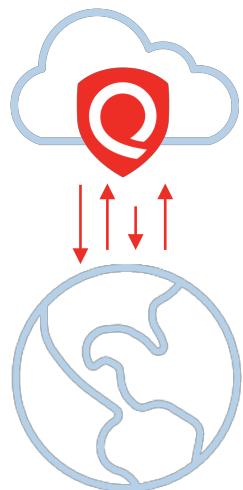
Provision Key for these applications

<input checked="" type="checkbox"/>  VM	Vulnerability Management 98919 Licenses Remaining	<input checked="" type="checkbox"/>  PC	Policy Compliance 99134 Licenses Remaining
<input type="checkbox"/>  FIM	File Integrity Monitoring 998 Licenses Remaining	<input type="checkbox"/>  IOC	Indication of Compromise 96 Licenses Remaining

Set limits

[Close](#) Unlimited Key 

Cloud Agent Extends Network Scanning



No scan windows needed – always collecting

Find vulnerabilities faster

Detect a fixed vulnerability faster

Many new Apps only available on Agent

Best for assets that can't be scanned

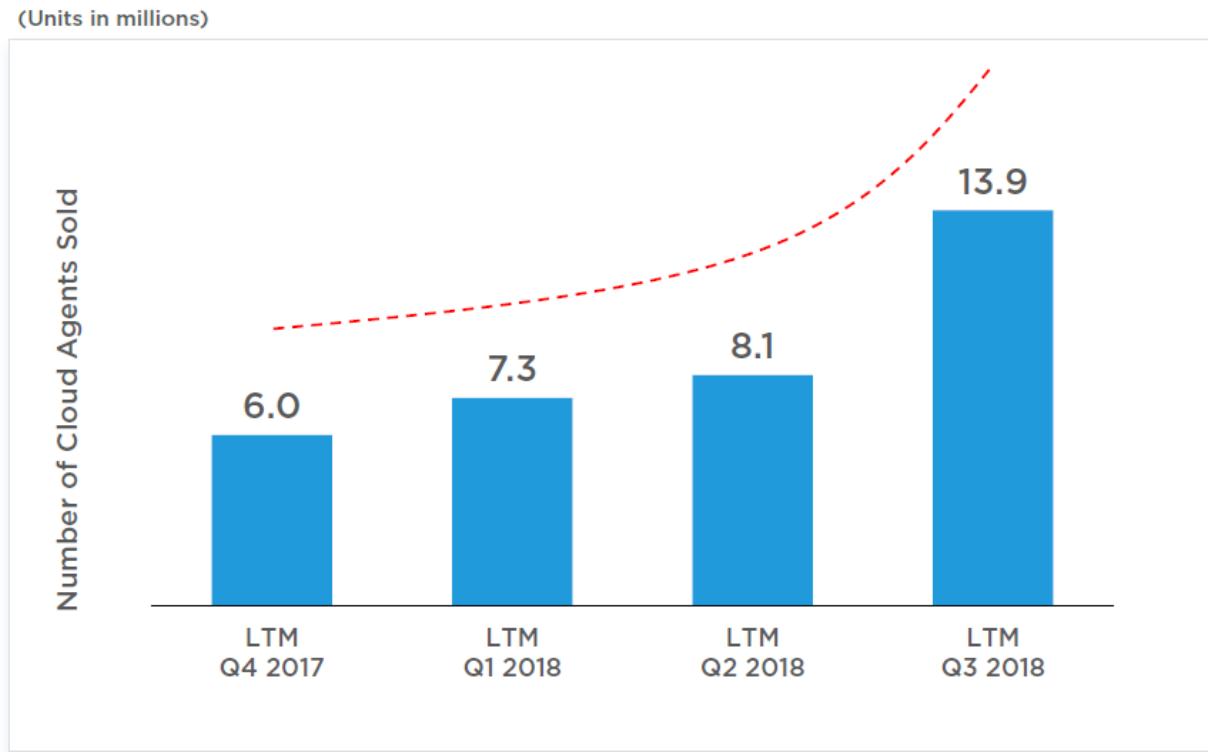
Unable to get credentials / authentication failures

Remote systems in branch offices / NAT

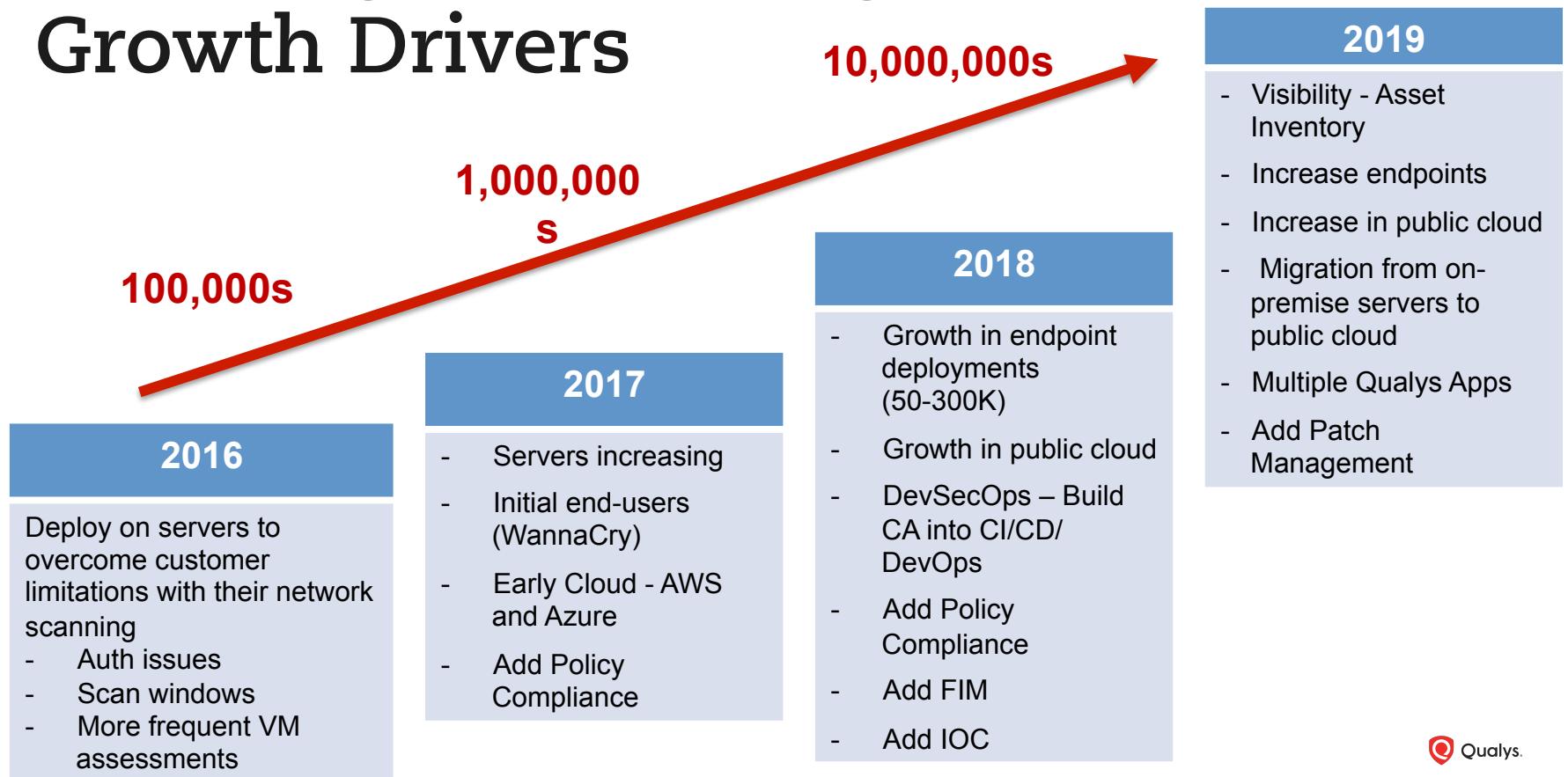
Roaming user endpoints

Cloud / Elastic deployments

Cloud Agent Adoption

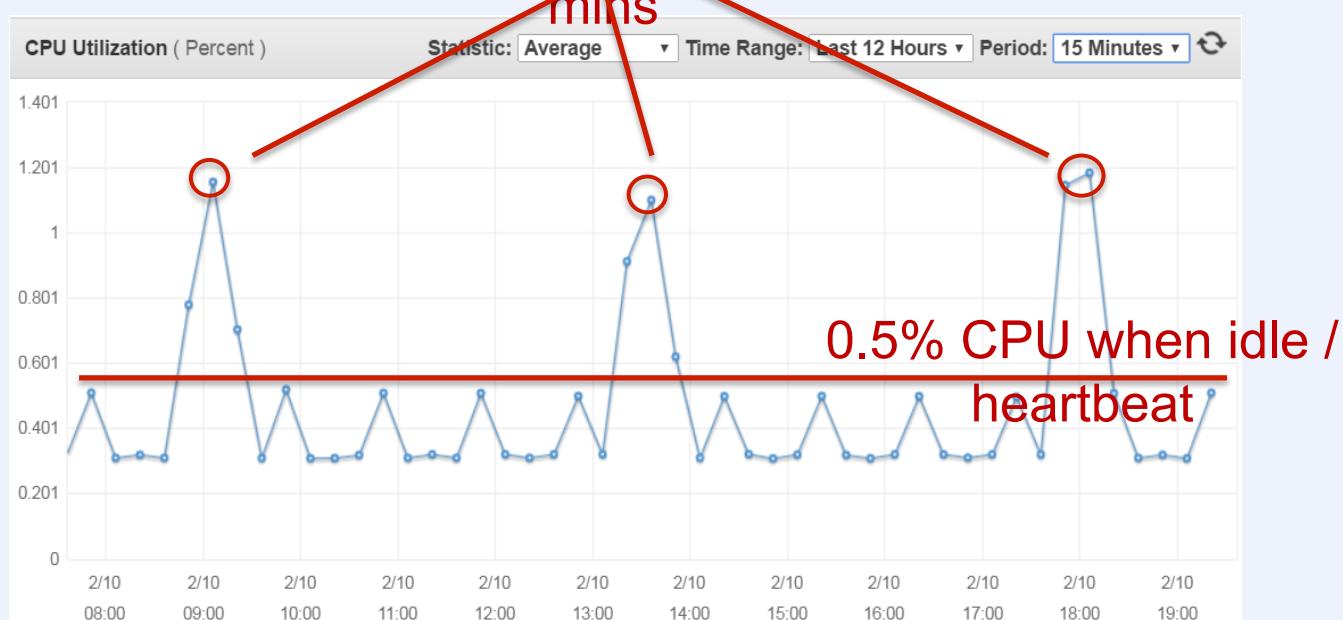


Cloud Agent VM Usage and Growth Drivers



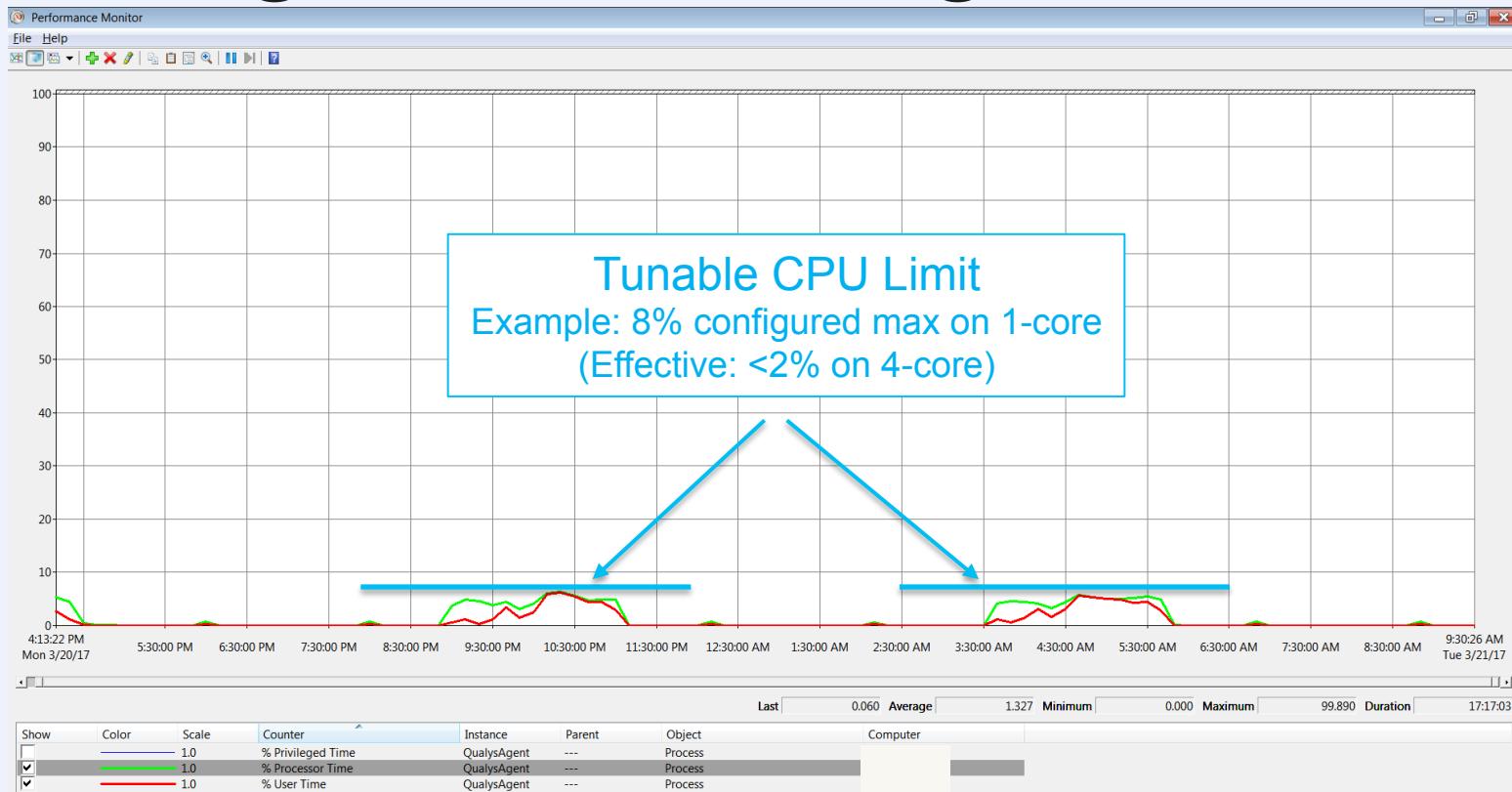
Cloud Agent CPU Tuning - Linux

AWS EC2
not allowed to
scan **nano**,
micro, or **small**
instances
using network
scanning



AWS t2.micro instance running Cloud Agent

Cloud Agent CPU Tuning - Windows



Cloud Native – Collect Provider Metadata

AWS EC2	Microsoft Azure	Google Compute Platform
accountId amiId availabilityZone hostname hostnamePublic instancetype instanceType kernelId macAddress privateIpAddress publicIpAddress region reservationId securityGroupIds securityGroups subnetId VPCId	dnsservers ipv6 location macAddress name offer osType privateIpAddress publicIpAddress publisher resourceGroupName tags subnet subscriptionId version vmlId vmSize	hostname instancetype macAddress machineType network privateIpAddress projectId projectIdNo publicIpAddress zone

Agent collects metadata locally

Cloud Provider Metadata

(AWS EC2 example)

accountId	383031258652
ami-id	ami-d874e0a0
ami-launch-index	2
availabilityZone	us-west-2a
hostname	ip-172-31-36-214.us-west-2.compute.internal
imageId	ami-d874e0a0
instance-id	i-03e86d77745bb2bba
instanceType	t2.micro
local-hostname	ip-172-31-36-214.us-west-2.compute.internal
local-ipv4	172.31.36.214
mac	06:26:0c:74:c5:9a
privateIp	172.31.36.214
profile	default-hvm
public-hostname	ec2-18-236-81-63.us-west-2.compute.amazonaws.com
public-ipv4	18.236.81.63
region	us-west-2
reservation-id	r-06e5580c2918a00ba
security-groups	launch-wizard-2

Cloud Instance Metadata Merge and Agent Dynamic License Management

EC2 Connector – Available now

aws.ec2.accountId
aws.ec2.availabilityZone
aws.ec2.hostname
aws.ec2.hostnamePublic
aws.ec2.imageId
aws.ec2.instanceId
aws.ec2.instanceState
aws.ec2.instanceType
aws.ec2.kernelId
aws.ec2.privateDNS
aws.ec2.privateIPAddress
aws.ec2.publicDNS
aws.ec2.publicIPAddress
aws.ec2.region.code
aws.ec2.region.name
aws.ec2.spotInstance
aws.ec2.subnetId
aws.ec2.VPCId

*Automatically merge
on Instance ID (Nov
2018)*

*Automated Rules (Dec
2018)*

*"When instanceState =
TERMINATED, then remove Cloud
Agent license"*

Cloud Agent – Available now

aws.ec2.accountId
aws.ec2.availabilityZone
aws.ec2.hostname
aws.ec2.imageId
aws.ec2.instanceId
aws.ec2.instanceType
aws.ec2.kernelId
aws.ec2.privateDNS
aws.ec2.privateIPAddress
aws.ec2.publicDNS
aws.ec2.publicIPAddress
aws.ec2.region.code
aws.ec2.region.name
aws.ec2.subnetId
aws.ec2.VPCId

Integrate Cloud Agent into DevOps



Use Cases for DevOps

Build Cloud Agent into gold image or auto-deploy with CI/CD – self-service results from Qualys API/UI & integrations

Get vulnerability and configuration posture of OS and application along the DevOps pipeline

Fix/verify security issues before going into production



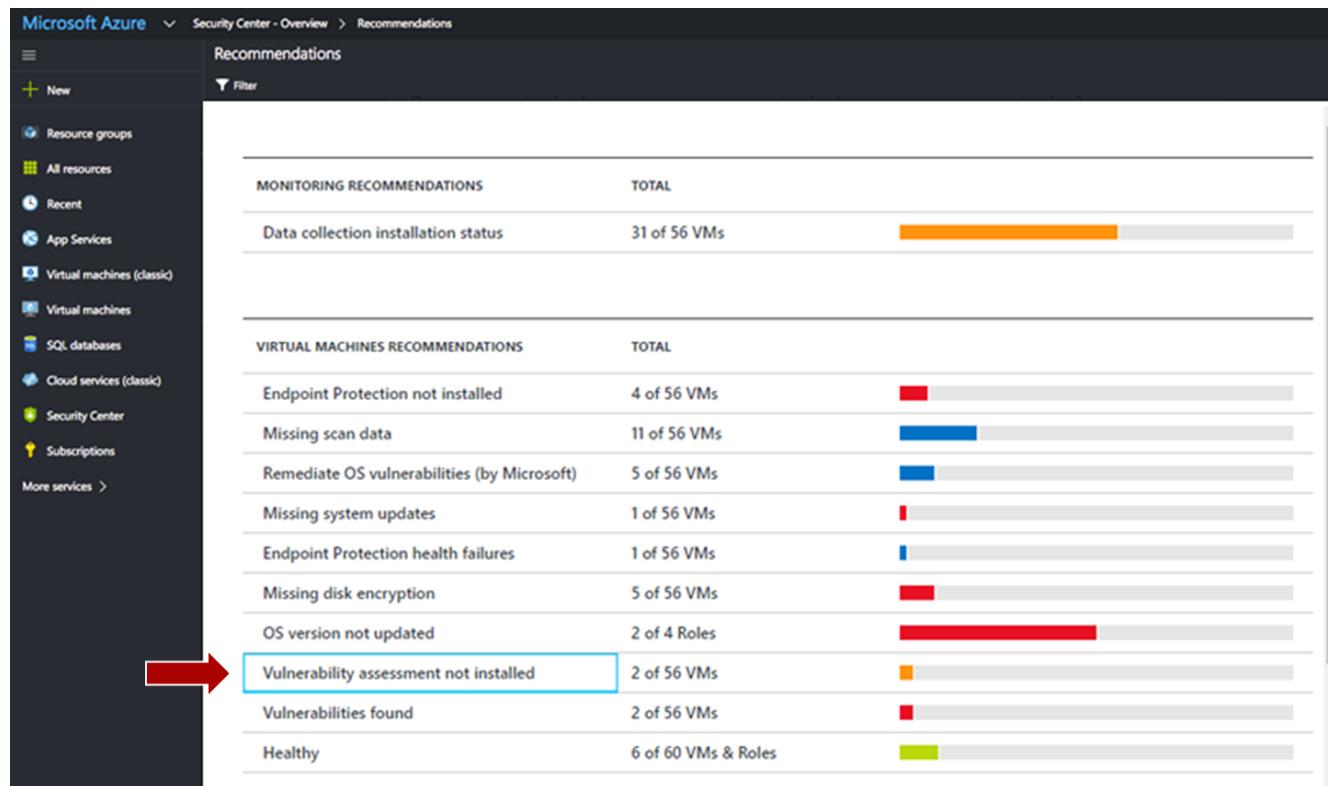
Use Cases for Security

End-to-end lifecycle tracking – development, deployment, production, decommission

Same Cloud Agent across cloud, on-premise, endpoint, hybrid

Single platform as DevOps tools evolve – Qualys Container Security, Jenkins integration, API automation, more

Cloud Agent – Microsoft Azure Integration



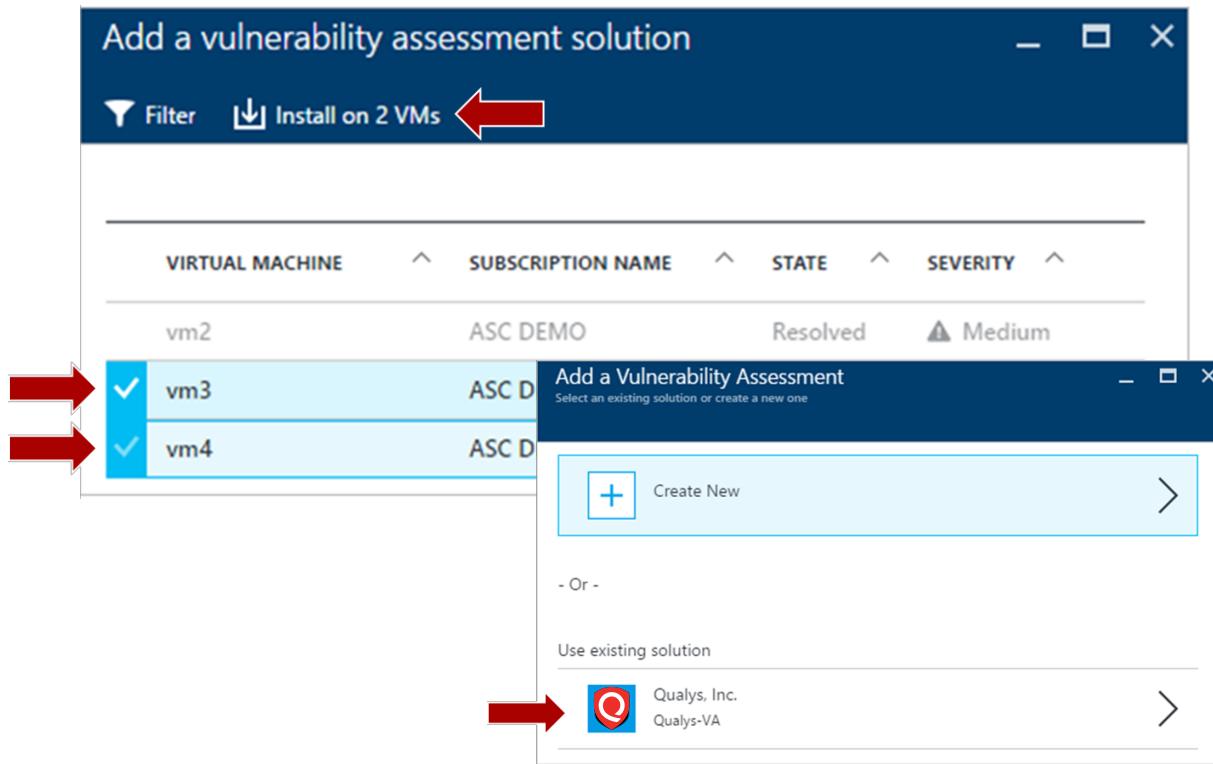
The screenshot shows the Microsoft Azure Security Center - Overview > Recommendations page. The left sidebar lists various Azure services like Resource groups, All resources, App Services, etc. The main area displays monitoring and virtual machine recommendations.

MONITORING RECOMMENDATIONS

	TOTAL
Data collection installation status	31 of 56 VMs

VIRTUAL MACHINES RECOMMENDATIONS

	TOTAL
Endpoint Protection not installed	4 of 56 VMs
Missing scan data	11 of 56 VMs
Remediate OS vulnerabilities (by Microsoft)	5 of 56 VMs
Missing system updates	1 of 56 VMs
Endpoint Protection health failures	1 of 56 VMs
Missing disk encryption	5 of 56 VMs
OS version not updated	2 of 4 Roles
Vulnerability assessment not installed	2 of 56 VMs
Vulnerabilities found	2 of 56 VMs
Healthy	6 of 60 VMs & Roles



RESOURCE GROUP	HS_RESOURCEGROUP			
SUBSCRIPTION	Visual Studio Premium with MSDN			
VIRTUAL IP				
OPERATING SYSTEM	Windows			
VERSION	Compute			
STATUS	Deallocated			
MONITORING STATE	Monitored by Azure Security Center			
PREVENTION STATUS	High severity			
Security Solutions				
SYSTEM UPDATES	Microsoft (Last scan time - 10/3/2016 1:22 PM)			
OS VULNERABILITIES	Microsoft (Last scan time - 10/3/2016 1:22 PM)			
VULNERABILITY SCANNER - PREVIEW	Qualys (Last scan time - 10/3/2016 11:56 PM)			
Recommendations				
DESCRIPTION	RESOURCE	STATE	SEVERITY	
Install Endpoint Protection	harivm2	Open	● High	...
Remediate vulnerabilities (by Qualys)	harivm2	Open	● High	...

VULNERABILITY NAME	VENDOR	AFFECT...	STATE	SEVERITY	
Enabled DCOM	Qualys	harivm2	Open	● High	...
Allowed Null Session	Qualys	harivm2	Open	▲ Medium	...
Enabled Cached Logon Cre...	Qualys	harivm2	Open	▲ Medium	...
Machine Information Disclo...	Qualys	harivm2	Open	▲ Medium	...
Microsoft Windows Explore...	Qualys	harivm2	Open	▲ Medium	...
Windows Explorer Autopla...	Qualys	harivm2	Open	▲ Medium	...
Access to File Share is Enab...	Qualys	harivm2	Open	● Low	...
ActiveX Controls Enumerated	Qualys	harivm2	Open	● Low	...
Antivirus Product Not Dete...	Qualys	harivm2	Open	● Low	...
Disabled Clear Page File	Qualys	harivm2	Open	● Low	...
Enabled Caching of Dial-up...	Qualys	harivm2	Open	● Low	...
Enabled Display Last Usern...	Qualys	harivm2	Open	● Low	...
File Access Permissions for ...	Qualys	harivm2	Open	● Low	...
File Access Permissions for ...	Qualys	harivm2	Open	● Low	...
Host Scan Time	Qualys	harivm2	Open	● Low	...
Hyper-V Host Information ...	Qualys	harivm2	Open	● Low	...
Installed Applications Enu...	Qualys	harivm2	Open	● Low	...
Internet Protocol version 6 ...	Qualys	harivm2	Open	● Low	...
IPSEC Policy Agent Service ...	Qualys	harivm2	Open	● Low	...
Message For Users Attempt...	Qualys	harivm2	Open	● Low	...



VULNERABILITY NAME	VENDOR	AFFECT...	STATE	SEVERITY	...
Enabled DCOM	Qualys	harivm2	Open	❗ High	...
Allowed Null Session	Qualys	harivm2	Open	⚠ Medium	...
Enabled Cached Logon Cre...	Qualys	harivm2	Open	⚠ Medium	...
Machine Information Disclo...	Qualys	harivm2	Open	⚠ Medium	...
Microsoft Windows Explore...	Qualys	harivm2	Open	⚠ Medium	...
Windows Explorer Autopla...	Qualys	harivm2	Open	⚠ Medium	...
Access to File Share is Enab...	Qualys	harivm2	Open	ℹ Low	...
ActiveX Controls Enumerated	Qualys	harivm2	Open	ℹ Low	...
Antivirus Product Not Dete...	Qualys	harivm2	Open	ℹ Low	...
Disabled Clear Page File	Qualys	harivm2	Open	ℹ Low	...

VULNERABILITY NAME

Enabled DCOM

SEVERITY

❗ High

DESCRIPTION

The Distributed Component Object Model (DCOM) is a protocol that enables software components to communicate directly over a network. The Distributed Component Object Model (DCOM) is enabled on this system.

SOLUTION

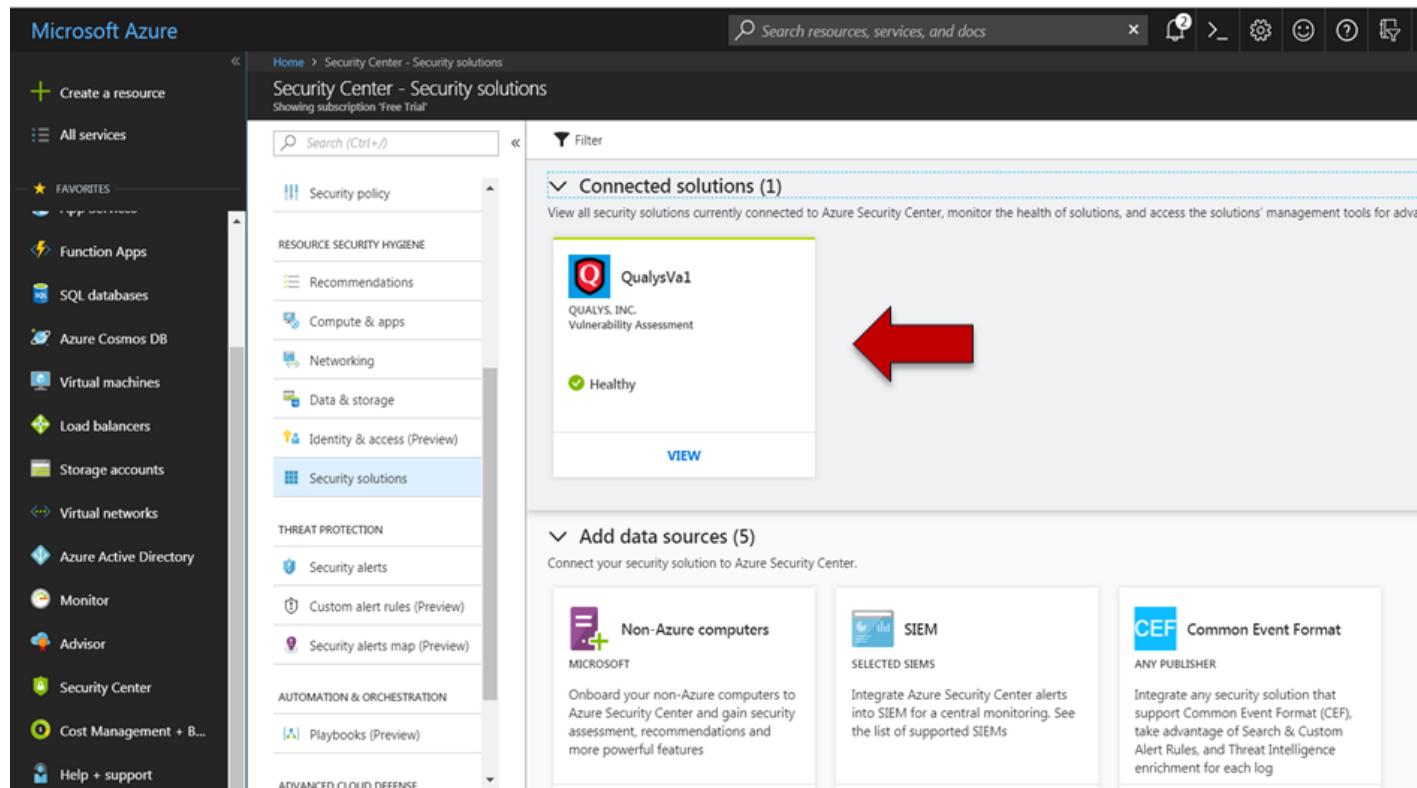
Refer to Microsoft article Best Practices for Mitigating RPC and DCOM Vulnerabilities to obtain information on vulnerabilities in DCOM and ways to mitigate those vulnerabilities. Information on disabling DCOM can be found at the Microsoft Technet article called How to Disable DCOM Support in Windows. For disabling DCOM on Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 refer to Microsoft's article Enable or Disable DCOM.

Vulnerability Spread at Speed of DevOps

The screenshot shows the Microsoft Azure Compute Virtual Machines interface. On the left, the navigation menu includes options like Create a resource, All services, Favorites, Resource groups, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, and Security Center. The main area displays a list of virtual machines under the 'Virtual machines' tab, with three entries visible: RHEL74-CC1-Azure, RHEL75-CC2-Azure, and RHEL75-CC3-USEast2-Azure. To the right, under the 'Compute' tab, there's a 'Recommended' section featuring icons for Windows Server (Microsoft), Red Hat Enterprise Linux (RedHat), Ubuntu Server (Canonical), and SQL Server 2017 Enterprise (Microsoft). The Red Hat Enterprise Linux icon is highlighted with a red box and a red arrow points from it to the text 'Red Hat 7.4 Marketplace Image' located on the right side of the slide.

Red Hat 7.4 Marketplace Image

Auto-Deploy Qualys Cloud Agent



The screenshot shows the Microsoft Azure Security Center - Security solutions page. On the left, there's a sidebar with various service icons like Function Apps, SQL databases, and Virtual machines. The main area shows a list of connected solutions under 'Connected solutions (1)'. One solution, 'QualysVa1' by QUALYS, INC., is listed as 'Healthy'. A red arrow points from the text below to this 'QualysVa1' entry. Below this section, there are other options like 'Add data sources (5)' and 'Non-Azure computers'.

Microsoft Azure

Home > Security Center - Security solutions

Search resources, services, and docs

Connected solutions (1)

QualysVa1

QUALYS, INC.

Vulnerability Assessment

Healthy

VIEW

Add data sources (5)

Non-Azure computers

MICROSOFT

Onboard your non-Azure computers to Azure Security Center and gain security assessment, recommendations and more powerful features

SIEM

SELECTED SIEMS

Integrate Azure Security Center alerts into SIEM for a central monitoring. See the list of supported SIEMs

CEF Common Event Format

ANY PUBLISHER

Integrate any security solution that support Common Event Format (CEF), take advantage of Search & Custom Alert Rules, and Threat Intelligence enrichment for each log

Vulnerability Results

RHEL74-CC1-Azure

View Mode

- Asset Summary
- System Information
- Agent Summary
- Network Information 
- Open Ports
- Installed Software
- Vulnerabilities** 
- Threat Protection RTIs
- File Integrity Monitoring
- Indication of Compromise
- Alert Notifications
- Azure VM Information

Vulnerabilities

Select the severity you would like to view by:

Severity Sev 5 Sev 4 Sev 3 Sev 2 Sev 1 [View vulnerabilities \(27\)](#)

Confirmed Vulnerabilities
24 [View](#)



Severity	Count
Sev 5	1
Sev 4	16
Sev 3	7
Sev 2	0
Sev 1	0

Potential Vulnerabilities
3 [View](#)



Severity	Count
Sev 5	0
Sev 4	0
Sev 3	3
Sev 2	0
Sev 1	0

Vulnerability Detection by Status

In the last

Status	Active	New	Reopened	Fixed
Confirmed	27	0	0	0
Potential	3	0	0	0

Close

Threat Protection Exploitability 😞

RHEL74-CC1-Azure

View Mode

- Asset Summary
- System Information →
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- Threat Protection RTIs
- File Integrity Monitoring
- Indication of Compromise
- Alert Notifications
- Azure VM Information

Threat Protection Summary

Total Vulnerabilities by RTIs **72**

RTI Type	Count
Zero Day	1
Easily Exploitable	22
Unpatchable	1
Active Attacks	1
Exploit Kit Available	0
High Lateral Movement	10
High Data Loss	13
Vulnerable to DOS	10
Malware	0
Public Exploit	14

LATEST THREATS FROM LIVE FEED

Title	Severity	Published
OpenSSH User name Enumeration Vulnerability : CVE-2018-15473	HIGH	8/29/2018
L1 Terminal Fault /Foreshadow Attack aka L1TF Attack	HIGH	8/28/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/28/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/22/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/20/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/20/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/15/2018
PoC Exploit available for CVE-2018-15473	MEDIUM	8/15/2018
SegmentSmack: CVE-2018-5390	HIGH	8/6/2018

Close

 Qualys.

Cloud Agent Roadmap

Agent Releases

- Mac 1.7.2 - released Aug 29
- Windows 2.1.1 - released Oct 22
- Linux 2.3 - Dec rollout for Policy Compliance UDCs
- <https://www.qualys.com/documentation/release-notes/>

Features

- Cloud Provider Metadata (AWS, Azure, GCP) – available
- EC2 Connector / Cloud Agent merge - available
- Nov - Windows agent to support Patch Management Beta
- Dec - Policy Compliance UDCs (Windows / Linux / AIX)
- Dec - Agent Lifecycle Management
(Public cloud State-based w/ Connector / Any asset using Time-based)



QUALYS SECURITY CONFERENCE 2018

Thank You

Chris Carlson

ccarlson@qualys.com



QUALYS SECURITY CONFERENCE 2018

Qualys Indication of Compromise

Bringing IOC to the Next Level

Chris Carlson

VP, Product Management, Qualys, Inc.

Adversary TTPs are Changing

Early 2010s

Zero-day Vulnerabilities

(Nation State, Industrial Espionage, Black Market)

Today

Rapidly weaponizing newly-disclosed vulnerabilities

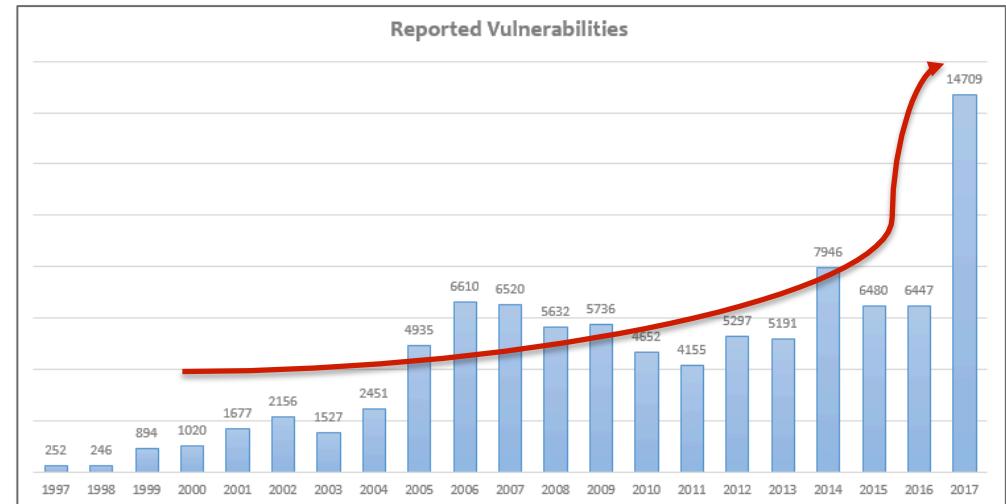
(Good, Fast, Cheap - Pick 3)

Known Critical Vulnerabilities are Increasing

6-7K vulnerabilities are disclosed each year*

30-40% are ranked as “High” or “Critical” severity

“Mean Time to Weaponize” (MTTW) is rapidly decreasing year-over-year



Announcing: CVE-2018-12238

Multiple Symantec Products CVE-2018-12238 Local Security Bypass Vulnerability

Bugtraq ID: 105917

CVE: CVE-2018-12238

Remote: No Local: Yes

Published: Nov 28 2018 12:00AM

Credit: Qualys Malware Research Lab

Vulnerable:

Symantec Norton AntiVirus 22.7

Symantec Norton AntiVirus 21.0

Symantec Norton AntiVirus 17.6.0.32

Symantec Endpoint Protection Cloud 12.1.6

Symantec Endpoint Protection Cloud 14

Symantec Endpoint Protection 12.1.6 MP4

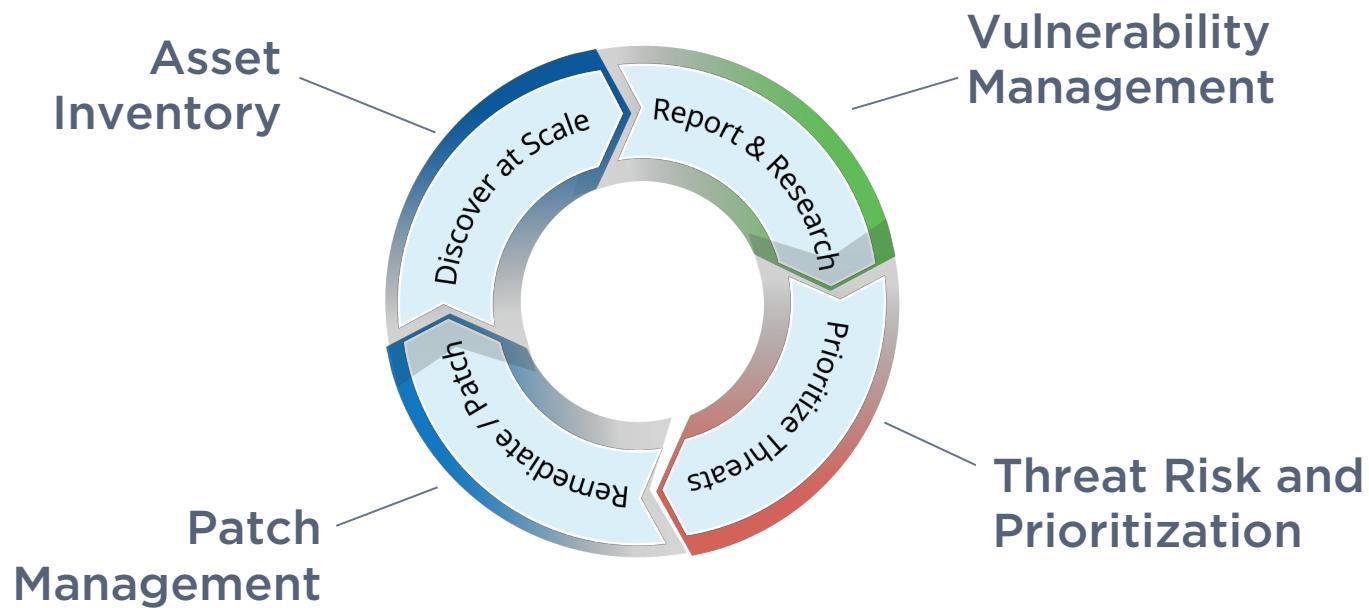
Symantec Endpoint Protection 12.1.6

+ 95 other products

QID 371337

QID 371338

Vulnerability Management Lifecycle



Get Proactive – Reduce the Attack Surface

Immediately Identify Vulnerabilities in Production

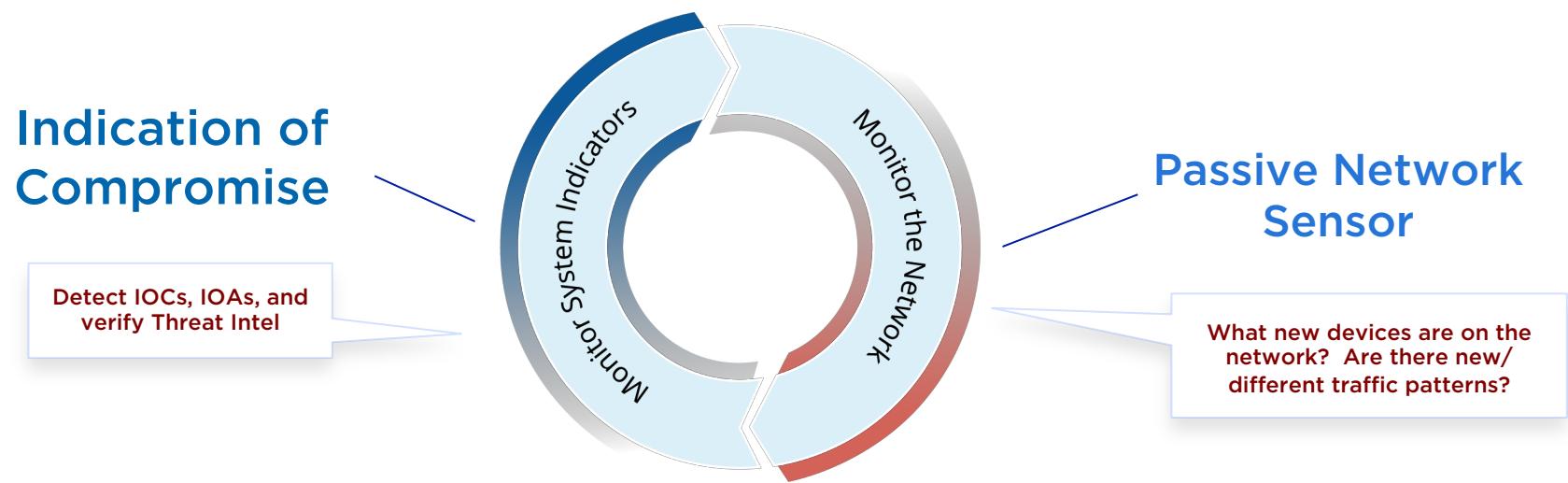
Notify IT Asset Owner to Patch/Stop the Instance

Control Network Access / Cloud Security Groups

Change Configuration to Limit Access (Compliance)

Add Detection and Response – Endpoint & Network

Proactively Hunt, Detect, and Respond



Organizations Struggle to Answer Basic Questions

Are these hashes on/running in my network?

Are these mutexes / processes / registry keys?

Did any endpoints connect to these IPs / Domains?

Are there any connections to TOR exit nodes?

What system is the first impacted? “*Patient Zero*”

Did this spread to others systems? When?

Qualys IOC Use Cases –

Visibility Beyond Anti-Virus

Threat Intel Verification

Threat Intel Feeds / Mandated to Verify
“Is this hash, registry, process, mutex on my
network?”

Hunting / Find Suspicious Activity

Indicator of Activity hunting with pre-built
and user-defined queries for Fileless attacks

“Look Back” Investigation after a known breach

Go back over months of stored events and
find the first occurrence of a breach

API
Integration
SIEM

Detect Known/Unknown Malware Family Variants

Using Qualys Malware Labs behavior models
and Threat Feeds (OEM, customer)

Threat Intel Verification

NotPetya Ransomware spreading using ETERNALBLUE Vulnerability and Credential Stealing
October 6, 2017

On June 27, 2017, NCCIC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list.

Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods using the ETERNALBLUE vulnerability and credential stealing via a modified version of Mimikatz.

Technical Details

Anti-Virus Coverage

VirusTotal reports 0/66 anti-virus vendors have signatures for the credential stealer as of the date of this report

Files

Delivery – MD5: 71b6a493388e7d0b40c83ce903bc6b04
Installation – MD5: 7e37ab34ecdcc3e77e24522ddfd4852d
Credential Stealer (new) – MD5: d926e76030f19f1f7ef0b3cd1a4e80f9

Secondary Actions

NotPetya leverages multiple propagation methods to spread within an infected network.
According to malware analysis, NotPetya attempts the lateral movement techniques below:

1 Threat Intelligence lists attack information ...

2 Search for the file hash here...

The screenshot shows the Qualys Enterprise Hunting interface. A red arrow points from the NotPetya MD5 hash (d926e76030f19f1f7ef0b3cd1a4e80f9) in the threat intel box to the search bar in the Qualys interface. Another red arrow points from the search result table to the object name "svvhost.exe".

TIME	OBJECT	ASSET	SCORE
a day ago 3:58:48 PM	svvhost.exe C:\14279270823	WIN2008R2-11566 10.11.114.113	
a day ago 12:22:57 PM	svvhost.exe C:\793972740527	WIN7-320860-T44 10.11.114.109	

3 Find the object there.

Malware Hides with Stolen Code-Signing Certificates



we live security™ BY eset

Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign

D-Link and Changing Information Technologies code-signing certificates stolen and abused by highly skilled cyberespionage group focused on East Asia, particularly Taiwan

<https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/>

IOC 2.0 Release (Dec 2018)

Responses - Alerting and Actions

Send alerts via Email, Slack, PagerDuty for any Hunting (QQL) searches

UI Updates

Event Relationship Tree / Trending Widgets / Event Group By Asset

Threat Feed (find malware that legacy AV may have missed)

Known Bad – 1B hashes

CVE-to-Malware hashes (shared with Threat Protection)

New Scoring Model

Prioritization for Investigation and Response (confirmed vs. suspicious)

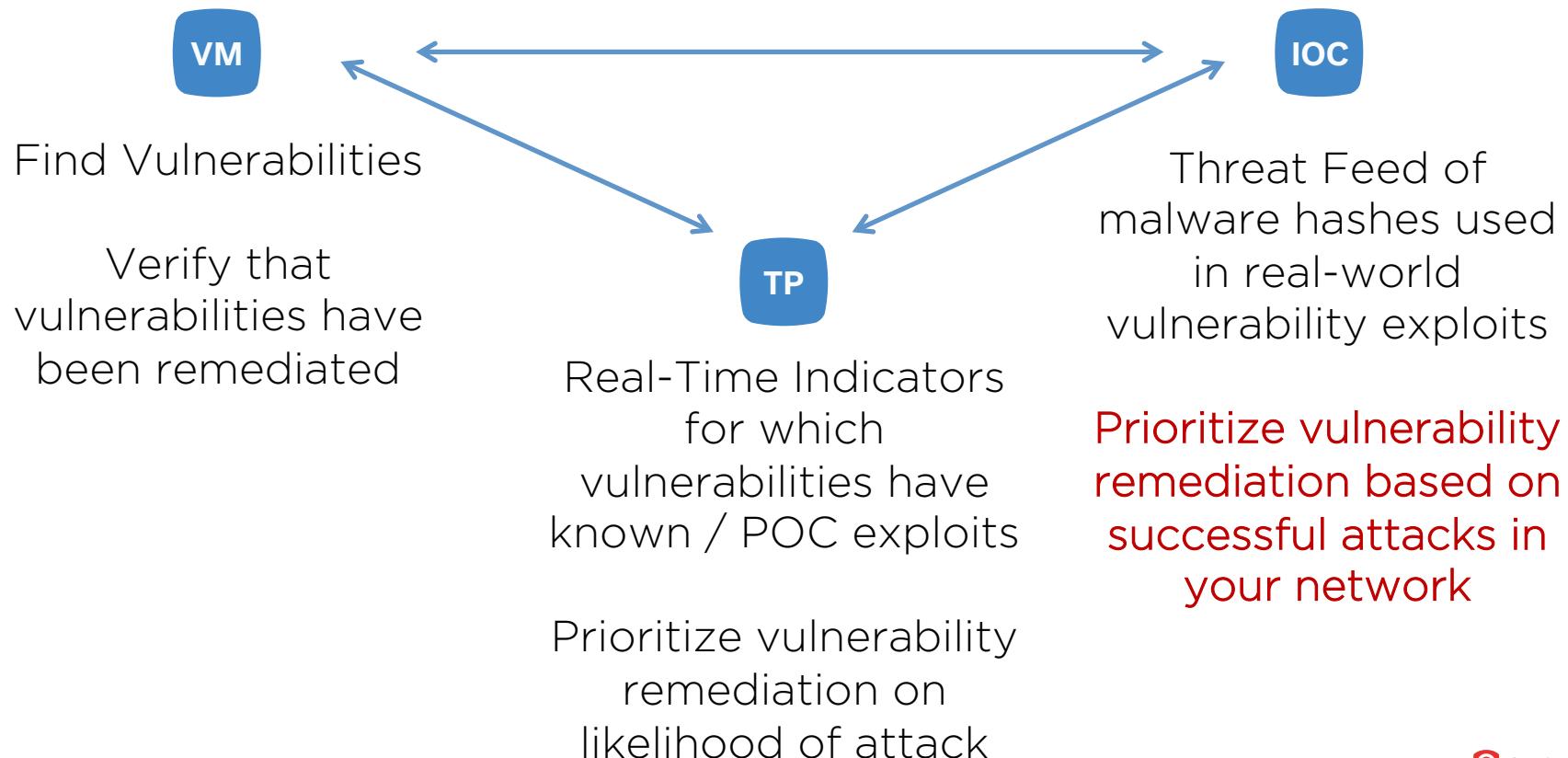
Integration with Alerting / Actions

IOC API

Integrate with any 3rd party SIEM / TIP

Splunk TA + Dashboards – Jan 2019

New IOC CVE - File Reputation Threat Feed



DEMO



Indication of Compromise

Threat Intel Verification

Hunting

Alerting

Create Emergency Patch Job from CVE Exploitation

18fc1b9b29a2d281ec9310f9f226ad77e3cb9c558f696c37390bbac72baa8ba8

168.63.129.16



QUALYS SECURITY CONFERENCE 2018

Thank You

Chris Carlson

ccarlson@qualys.com